

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application )

Applicant: Omote et al. )

Serial No. )

Filed: March 30, 2004 )

For: DEVICE AND METHOD FOR WORM )  
DETECTION, AND COMPUTER )  
PRODUCT )

Art Unit: )

*I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.*

March 30, 2004  
DateDail Aman  
Express Mail Label No.: EV032736278USCLAIM FOR PRIORITY

Mail Stop PATENT APPLICATION  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

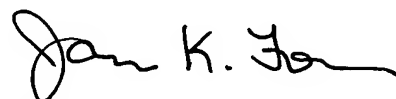
Japanese Patent Application No. 2003-367272, filed October 28, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By



James K. Folker

Registration No. 37,538

**Customer No. 24978**

March 30, 2004  
300 South Wacker Drive - Suite 2500  
Chicago, Illinois 60606  
Phone: (312) 360-0080  
Fax: (312) 360-9315

1924.70199  
(312) 360-0080日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年 1 0 月 2 8 日  
Date of Application:

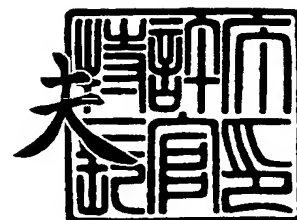
出 願 番 号                      特 願 2 0 0 3 - 3 6 7 2 7 2  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 3 6 7 2 7 2 ]

出 願 人                      富士通株式会社  
Applicant(s):

2 0 0 4 年    2 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 4 - 3 0 1 0 6 4 5



【書類名】 特許願  
【整理番号】 0352422  
【提出日】 平成15年10月28日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 11/30  
【発明者】  
    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社  
                        内  
    【氏名】 面 和成  
【発明者】  
    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社  
                        内  
    【氏名】 鳥居 悟  
【特許出願人】  
    【識別番号】 000005223  
    【氏名又は名称】 富士通株式会社  
【代理人】  
    【識別番号】 100089118  
    【弁理士】  
    【氏名又は名称】 酒井 宏明  
【手数料の表示】  
    【予納台帳番号】 036711  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9717671

**【書類名】 特許請求の範囲****【請求項 1】**

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させることを特徴とするワーム判定プログラム。

**【請求項 2】**

前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする請求項 1 に記載のワーム判定プログラム。

**【請求項 3】**

前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする請求項 2 に記載のワーム判定プログラム。

**【請求項 4】**

前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする請求項 1、2 または 3 に記載のワーム判定プログラム。

**【請求項 5】**

前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする請求項 1～4 のいずれか 1 つに記載のワーム判定プログラム。

**【請求項 6】**

前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする請求項 5 に記載のワーム判定プログラム。

**【請求項 7】**

前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする請求項 5 に記載のワーム判定プログラム。

**【請求項 8】**

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 9】

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、

前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、

を含んだことを特徴とするワーム判定方法。

【請求項 10】

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、

前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、

を備えたことを特徴とするワーム判定装置。

**【書類名】明細書**

**【発明の名称】** ワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置

**【技術分野】****【0001】**

この発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置に関し、特に、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置に関するものである。

**【背景技術】****【0002】**

近年、自己増殖を繰り返しながらコンピュータに次々と感染し、コンピュータに悪影響を及ぼすワームと呼ばれるコンピュータウイルスによる被害が拡大してきている。古くは、ワームは、フレキシブルディスク（FD）やCD-ROMなどを介してコンピュータに感染していたため感染力がそれほど大きくはなかったが、最近では、インターネットが普及するにつれワームの感染力が加速度的に大きくなり、ワームに対する防御をいかにこなうかが大きな問題となっている。

**【0003】**

そのため、特許文献1には、ワームを含んでいるかどうかを検査する検査対象を仮想的に構築したコンピュータ環境に導入し、その検査対象が仮想的なコンピュータ環境における所定のファイルを変更するか否かを監視することにより、ワームであるか否かを判定するワームの検査方法が開示されている。

**【0004】**

また、非特許文献1には、ワームにより攻撃された場合に必ず生じるサーバ装置の振る舞い（データI/Oやシステムコールなどの系列）をあらかじめ監視ルールとして定義しておき、ワームを含んでいるかどうかを検査する検査対象をアクセス検査サーバ装置に導入して、その動作を監視することによりワームによる攻撃を検出するWebサーバ防御システムが開示されている。

**【0005】**

**【特許文献1】** 特開2002-342106号公報

**【非特許文献1】** 日本電気株式会社、“プレスリリース”、[online]、2003年4月11日、[平成15年10月28日検索]、インターネット<URL: <http://www.nec.co.jp/press/ja/0304/1101.html>>

**【発明の開示】****【発明が解決しようとする課題】****【0006】**

しかしながら、上記特許文献1の従来技術では、通信をおこなう度に検査対象をあらかじめ構築しておいた仮想的なコンピュータ環境に導入し、その仮想的なコンピュータ環境に対する感染の有無を検査する必要があるため、すべての通信に関してワームの検出をおこなうのは効率的でなく、ワームを含んでいる危険性のある通信のみに対して検査をおこなうにしても、その危険性を判定する基準を定めることが難しいという問題があった。

**【0007】**

また、非特許文献2の従来技術では、ワームにより攻撃された場合に必ず生じるサーバ装置の振る舞いを監視ルールとして定義しておくこととしているが、多くの用途に使用され、さまざまな振る舞いを示すクライアント装置に対して、ワーム攻撃による振る舞いと通常使用による振る舞いとを区別する監視ルールを定義することが難しいという問題があ

った。

【0008】

この発明は、上述した従来技術による問題点を解消するためになされたものであり、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置を提供することを目的とする。

【課題を解決するための手段】

【0009】

上述した課題を解決し、目的を達成するため、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、をコンピュータに実行させることを特徴とする。

【0010】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記情報の取得に係る設定情報を変更する設定情報変更手順をさらに含み、前記通信情報取得手順は、前記情報取得設定変更手順により変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得することを特徴とする。

【0011】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記判定基準に係る情報を変更する判定基準情報変更手順をさらに含み、前記ワーム判定手順は、前記通信情報取得手順により取得された情報および前記判定基準情報変更手順により変更された判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定することを特徴とする。

【0012】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのバケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする。

【0013】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする。

【0014】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのバケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータ

からの通信がワームによりなされた通信であると判定することを特徴とする。

【0015】

また、本発明は、前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、該通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することを特徴とする。

【0016】

また、本発明は、前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされた通信に係る特徴とを比較することにより前記ワームの種類を推定することを特徴とする。

【0017】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする。

【0018】

また、本発明は、前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする。

【0019】

また、本発明は、前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする。

【0020】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とする。

【0021】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、を含んだことを特徴とする。

【0022】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、を備えたことを特徴とする。

【発明の効果】

【0023】

本発明によれば、情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、取得された情報および通信がワームによ



りなされた通信か否かを規定する判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるという効果を奏する。

【0024】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、情報の取得に係る設定情報を変更し、変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得することとしたので、通信がワームによりなされた通信と判定された場合に情報の取得に係る設定情報を変更することにより、さらに詳細にワームの挙動を監視することができるという効果を奏する。

【0025】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、判定基準に係る情報を変更し、取得された情報および変更された判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、通信がワームによりなされた通信と判定された場合に判定基準に係る情報を変更することにより、さらに厳密に通信がワームによりなされた通信か否かを判定することができるという効果を奏する。

【0026】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、通信パケットの宛先アドレス数が増加した場合に、所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント内のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【0027】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、通信がワームによりなされた通信であると判定する際に取得された所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント内の複数のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【0028】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメントに対してその所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、通信パケットの送信元アドレス数が増加した場合に、所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント外のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【0029】

また、本発明によれば、通信をワームによりなされた通信と判定した場合に、通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することとしたので、出力されたコンピュータに係る情報を基にしてワームに感染している可能性のあるコンピュータを特定することができるという効果を奏する。

【0030】

また、本発明によれば、通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされた通信と判定した通

信に係る特徴とを比較することによりワームの種類を推定することとしたので、推定されたワームの種類の情報に基づいてワームの攻撃に適切に対応することができるという効果を奏する。

【0031】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、ワームによりなされる通信を遮断することとしたので、ワームの増殖を効果的に抑制することができるという効果を奏する。

【0032】

また、本発明によれば、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することとしたので、ワームがおこなう処理自体を停止させることにより、ワームの増殖を効果的に抑制することができるという効果を奏する。

【0033】

また、本発明によれば、ワームによりなされる通信をワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することとしたので、ワームによりなされる通信をワームに感染しているコンピュータに遮断させることにより、ワームの増殖を効果的に抑制することができるという効果を奏する。

【発明を実施するための最良の形態】

【0034】

以下に添付図面を参照して、この発明に係るワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置の好適な実施の形態を詳細に説明する。

【実施例】

【0035】

まず、本実施例に係るネットワークセグメントの概念について説明する。図16は、本実施例に係るネットワークセグメントの概念を説明する概念図である。図16に示すように、本実施例におけるネットワークセグメントは、複数の階層からなる構造を有している。

【0036】

たとえば、最も小規模なネットワークセグメント16aは、ワーム判定プログラムが導入されたコンピュータを1台だけ含むものである。この場合、そのコンピュータがネットワークセグメント16aに係る通信を監視してワーム判定処理をおこなう。それよりもやや大きい規模のネットワークセグメント16bは、部署のイントラネット単位で構成されるセグメントであり、そのネットワークセグメント16bに対してワーム判定装置17aが接続され、そのワーム判定装置17aが、ワークセグメント16bに係る通信を監視してワーム判定処理をおこなう。

【0037】

さらに大きい規模であるネットワークセグメント16cは、企業のイントラネット単位で構成されるセグメントであり、そのネットワークセグメント16cに対してワーム判定装置17bが接続され、そのワーム判定装置17bが、ワークセグメント16cに係る通信を監視してワーム判定処理をおこなう。そして、より大規模のネットワークセグメント16dは、ISP (Internet Service Provider) 単位で構成されるセグメントであり、そのネットワークセグメント16dに対してワーム判定装置17cが接続され、そのワーム判定装置17cが、ワークセグメント16dに係る通信を監視してワーム判定処理をおこなう。

【0038】

このように、ネットワークセグメントの規模および形態には様々なものが考えられ、そのさまざまな規模および形態のネットワークセグメントに対して、本発明に係るワーム判定システムの適用をおこなうことができる。

【0039】

つぎに、本実施例に係るワーム判定システムの概念について説明する。図1は、本実施

例に係るワーム判定システムの概念について説明する概念図である。図1に示すように、このワーム判定システムは、サーバ装置やクライアント装置などを少なくとも1台以上含むネットワークセグメント10a~10dが、ワーム判定装置20a~20dを介してネットワーク11に接続された構成となっている。ここで、ネットワーク11とは、インターネット、イントラネット、ISPのネットワークなどを指している。

#### 【0040】

このワーム判定装置20a~20dは、各ネットワークセグメント10a~10dに他のネットワークセグメント10a~10dから送信される通信パケットと、各ネットワークセグメント10a~10dが他のネットワークセグメント10a~10dに送信する通信パケットとを監視して、その通信パケットによる通信がワームによりなされた通信であるか否かを判定する処理をおこなう。

#### 【0041】

具体的には、通信パケットの単位時間当たりのパケット数、各通信パケットの送信元IPアドレスおよび宛先IPアドレスの情報などを取得し、取得した情報に基づいて監視対象としているネットワークセグメント10a~10d外からのワームの攻撃があるか否かや、そのネットワークセグメント10a~10d内から他のネットワークセグメント10a~10d内のコンピュータに対してワームの攻撃がなされているか否か等を判定する。

#### 【0042】

ここで、ワームに感染した場合に生じる通信パケットの単位時間当たりのパケット数、各通信パケットの送信元IPアドレスおよび宛先IPアドレスの情報の変化は、サーバ装置やクライアント装置などのコンピュータの種類に依らず顕著に現れるため、このワーム判定システムにおいては、サーバ装置かクライアント装置かに拘らず容易にかつ効率的にワームを検出することができる。

#### 【0043】

また、ワームの特徴をあらかじめ登録しておき、その特徴を参照してワームによる通信を検出するのではなく、通信パケットの単位時間当たりのパケット数、各通信パケットの送信元IPアドレスおよび宛先IPアドレスの情報の変化を基にしてワームによる通信か否かを判定するので、未知のワームに対しても適切に対処することができる。

#### 【0044】

つぎに、本実施例に係るワーム判定装置20a~20dの機能的構成について説明する。図2は、本実施例に係るワーム判定装置20a~20dの機能的構成について説明する機能ブロック図である。各ワーム判定装置20a~20dは、同様の機能を有するので、ここでは、ワーム判定装置20aの機能的構成について説明する。

#### 【0045】

図2に示すように、このワーム判定装置20aは、ネットワークセグメントA10aおよびネットワークセグメントA10aを除いたネットワーク12にLAN21およびネットワーク21を介して接続されている。ここで、LAN21は、イントラネットなどのネットワークである。

#### 【0046】

ワーム判定装置20aは、本発明に係る装置であり、情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、取得した情報と、通信がワームによりなされた通信か否かを規定する判定基準に係る情報とに基づいて通信がワームによりなされた通信か否かを判定する判定装置である。

#### 【0047】

このワーム判定装置20aは、インターフェース部200、入力部210、表示部220、記憶部230および制御部240を有する。インターフェース部200は、ネットワークセグメントA10aとネットワークセグメントAを除くネットワーク12との間の通信データの授受を、LAN21およびネットワーク21を介して中継するネットワークインターフェースである。

#### 【0048】

入力部 210 は、キーボードやマウスなどの入力デバイスであり、表示部 220 は、ディスプレイなどの表示デバイスである。記憶部 230 は、ハードディスク装置などの記憶デバイスであり、この記憶部 230 には、設定データ 230 a、通信ログデータ 230 b およびワームデータ 230 c が記憶されている。

【0049】

設定データ 230 a は、通信パケットの通信量および通信パケットの通信アドレスに係る情報の取得に係る設定情報や、監視している通信がワームによりなされた通信か否かを規定する判定基準に係る情報など、さまざまな設定情報を記憶したデータである。

【0050】

図 3 は、図 2 に示した設定データ 230 a の一例を示す図である。この設定データ 230 a は、設定項目、初期設定および SYN パケット異常検知後の設定の各項目を有する。設定項目は、設定データ 230 a において設定される各項目であり、初期設定は、通常監視時に参照される設定情報であり、SYN パケット異常検知後の設定は、監視していた SYN パケットに異常が検知された場合に、初期設定の代わりに参照される設定情報である。この SYN パケットの異常は、後に説明するように、単位時間内に計測した SYN パケットの数が所定の閾値以上で、宛先 IP アドレス数が所定の閾値以上となった場合を意味している。

【0051】

上記設定項目には、具体的には、SYN パケットの計測単位時間、SYN ACK パケットの計測単位時間、UDP パケットの計測単位時間、ICMP (request) パケットの計測単位時間、ICMP (reply) パケットの計測単位時間、宛先 IP アドレスの計測単位時間、送信元 IP アドレスの計測単位時間、宛先ポート番号の参照、SYN パケット数の閾値、SYN ACK パケット数の閾値、UDP パケットの閾値、ICMP (request) パケットの閾値、ICMP (reply) パケットの閾値、宛先 IP アドレス数の閾値、送信元 IP アドレス数の閾値、監視場所、監視するネットワークの方向、遮断および検知から遮断までの時間が登録されている。

【0052】

SYN パケットの計測単位時間、SYN ACK パケットの計測単位時間、UDP パケットの計測単位時間、ICMP (request) パケットの計測単位時間および ICMP (reply) パケットの計測単位時間は、それぞれ、TCP (Transmission Control Protocol) ベースのパケットである SYN パケット、SYN パケットをコンピュータが受信した際の応答として送信される SYN ACK パケット、UDP (User Datagram Protocol) ベースのパケットである UDP パケット、相手コンピュータの動作確認メッセージを送信する ICMP (Internet Control Message Protocol) (request) パケット、その ICMP (request) パケットの応答として送信される ICMP (reply) パケットの数を計測する単位時間である。たとえば、この単位時間が 1 sec であるということは、1 秒間の上記パケットの送信数または受信数を 1 秒ごとに計測することを意味する。

【0053】

また、宛先 IP アドレスの計測単位時間および送信元 IP アドレスの計測単位時間は、上記各パケットの宛先 IP アドレスおよび送信元 IP アドレスを計測する単位時間である。たとえば、この単位時間が 1 sec であるということは、1 秒間の上記パケットの宛先 IP アドレスおよび送信元 IP アドレスを 1 秒ごとに計測することを意味する。宛先ポート番号の参照は、上記各パケットの宛先ポート番号をリアルタイムで参照するか否かを設定する項目であり、「ON」または「OFF」のいずれかに設定される。

【0054】

SYN パケット数の閾値、SYN ACK パケット数の閾値、UDP パケットの閾値、ICMP (request) パケットの閾値、ICMP (reply) パケットの閾値は、ワームによりなされた通信がおこなわれているか否かを判定する際に使用されるパケッ

ト数の閾値情報である。宛先 IP アドレス数の閾値および送信元 IP アドレス数の閾値は、ワームによりなされた通信がおこなわれているか否かを判定する際に使用される宛先 IP アドレス数および送信元 IP アドレス数の閾値情報である。ここで、宛先 IP アドレス数または送信元 IP アドレス数は、宛先 IP アドレスの計測単位時間または送信元 IP アドレスの計測単位時間内に計測された異なる宛先 IP アドレスまたは送信元 IP アドレスの数である。

#### 【0055】

監視場所は、パケットを監視するネットワークドライバを設定する項目であり、たとえば、ネットワークドライバ「E t h 0」などと設定する。監視するネットワークの方向は、監視するパケット通信の方向を設定する項目である。たとえば、ワーム判定装置 20 a が接続されているネットワークセグメント A 10 a から外に送信されるパケットのみを監視する場合には、「O u t g o i n g」に設定され、ネットワークセグメント A を除くネットワーク 12 からネットワークセグメント A 10 a に対して送信されるパケットを監視する場合には、「i n c o m i n g」に設定され、それら両方のパケットを監視する場合には、「b o t h」に設定される。

#### 【0056】

遮断は、パケット通信がワームによりなされた通信と判定された場合に、通信の遮断をおこなうか否かを設定する項目であり、「ON」または「OFF」のいずれかに設定される。検知から遮断までの時間は、ワームによりなされたパケット通信を検知した場合に、パケット通信を遮断するまでの待ち時間を設定する項目であり、たとえば、「5 s e c」などと設定される。

#### 【0057】

図 2 の説明に戻ると、通信ログデータ 230 b は、パケット通信の通信記録を記憶したデータである。具体的には、図 3 で示した設定データ 230 a に基づいて取得された通信パケットのパケット数や IP アドレス数の情報、ワームによりなされた通信か否かを判定した判定結果の情報などを記憶している。

#### 【0058】

図 4 は、図 2 に示した通信ログデータ 230 b の一例を示す図である。図 4 に示すように、この通信ログデータ 230 b は、計測時間、パケット数および IP アドレス数の各項目を有する。計測時間は、計測をおこなった時間であり、パケット数は、各計測時間において計測されたパケット数である。このパケット数は、さらに、SYN パケット数、SYN ACK パケット数、UDP パケット数、ICMP (r e q u e s t) パケット数および ICMP (r e p l y) パケット数の項目を有し、各パケットの種類ごとに計測されたパケット数が記憶される。

#### 【0059】

IP アドレス数は、各計測時間において計測された IP アドレス数である。この IP アドレス数は、さらに、宛先 IP アドレス数および送信元 IP アドレス数の項目を有し、各計測時間における通信パケットの宛先 IP アドレス数および送信元 IP アドレス数の情報が記憶される。

#### 【0060】

また、図 3 に示した設定データ 230 a の「宛先ポート番号の参照」の項目が「ON」である場合には、通信ログデータ 230 b に、通信情報取得部 240 a により取得された最頻出宛先ポート番号の情報が各計測時間ごとに記憶される（図 4 には、図示せず。）。さらに、この通信ログデータ 230 b には、ワームによる通信がおこなわれたと判定された場合に、ワームの通信方法や通信速度、通信特徴が類似しているワームの情報などとともにその判定結果が記憶される（図 4 には、図示せず。）。

#### 【0061】

図 2 の説明に戻ると、ワームデータ 230 c は、ワームによりなされる通信の特徴を記憶したデータである。具体的には、このワームデータ 230 c は、過去に発見されたワームが単位時間内に他のコンピュータのスキャンをおこなうスキャン速度の情報や、攻撃す

る宛先ポート番号などのワームの特徴情報を記憶する。

#### 【0062】

制御部 2 4 0 は、ワーム判定装置 2 0 a を全体制御する制御部である。この制御部 2 4 0 は、通信情報取得部 2 4 0 a、ワーム判定部 2 4 0 b、設定データ変更部 2 4 0 c および通信遮断部 2 4 0 d を有する。

#### 【0063】

通信情報取得部 2 4 0 a は、記憶部 2 3 0 に記憶された設定データ 2 3 0 a に基づいて、通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得する取得部である。具体的には、この通信情報取得部 2 4 0 a は、通信パケットのパケット数を計測するとともに、通信パケットのヘッダから宛先 I P アドレスや送信元 I P アドレスの情報を取得し、宛先 I P アドレス数や送信元 I P アドレス数を計測したり、通信パケットの宛先ポート番号などの情報から最頻出宛先ポート番号の情報を取得したりして、通信ログデータ 2 3 0 b に記憶する処理などをおこなう。

#### 【0064】

ワーム判定部 2 4 0 b は、通信情報取得部 2 4 0 a により取得された情報、および、記憶部 2 3 0 に記憶された設定データ 2 3 0 a に基づいて、監視対象としているパケット通信がワームによりなされた通信か否かを判定する判定部である。つぎに、この判定処理の内容を具体的に説明する。

#### 【0065】

図 5 は、図 2 に示したワーム判定部 2 4 0 b がおこなうパケットの種類ごとのワーム判定処理の例を示す図である。図 5 では、ワーム判定部 2 4 0 b がおこなう判定処理の内容を 3 つのケースに分けて示している。ケース 1 は、O u t g o i n g 通信を監視している際に、S Y N パケット数が増加し、かつ、宛先 I P アドレス数が増加したという状況が観測された場合である。

#### 【0066】

この状況は、ネットワークセグメント A 1 0 a 外のさまざまなコンピュータに S Y N パケットが多数送信されていることを意味するので、ワーム判定部 2 4 0 b は、T C P ベースのワームがネットワークセグメント A 1 0 a 内のコンピュータに感染しており、ネットワークセグメント A 1 0 a 外のコンピュータに対してランダムスキャンをおこなっていると判定する。この場合、ワーム判定部 2 4 0 b は、さらに宛先ポート番号を計測し、最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する。たとえば、計測された最頻出宛先ポート番号が 8 0 番であれば、W e b サービスを狙ったワームであると判定できる。

#### 【0067】

ケース 2 は、O u t g o i n g 通信を監視している際に、U D P パケット数が増加し、かつ、宛先 I P アドレス数が増加したという状況が観測された場合である。この状況は、ネットワークセグメント A 1 0 a 外のさまざまなコンピュータに U D P パケットが多数送信されていることを意味するので、ワーム判定部 2 4 0 b は、U D P ベースのワームがネットワークセグメント A 1 0 a 内のコンピュータに感染しており、ネットワークセグメント A 1 0 a 外のコンピュータに対してランダムスキャンをおこなっていると判定する。この場合、ワーム判定部 2 4 0 b は、さらに宛先ポート番号を計測し、最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する。たとえば、計測された最頻出宛先ポート番号が 5 3 番であれば、D N S サービスを狙ったワームであると判定できる。

#### 【0068】

ケース 3 は、O u t g o i n g 通信を監視している際に、I C M P ( r e q u e s t ) パケット数が増加し、かつ、宛先 I P アドレス数が増加したという状況が観測された場合である。この状況は、ネットワークセグメント A 1 0 a 外のさまざまなコンピュータに I C M P ( r e q u e s t ) パケットが多数送信されていることを意味する。この場合、ワーム判定部 2 4 0 b は、パケットの送信がワームによるものか否かの判定を一時保留する。これは、I C M P ( r e q u e s t ) パケットは、相手コンピュータの動作確認メッセ

ージを送信するパケットであり、ICMP (request) パケットのパケット数および宛先 IP アドレス数が増加しただけでは、ワームによるランダムスキャンがおこなわれているのかが不明なためである。

#### 【0069】

この場合、ワーム判定部 240b は、その後送信される SYN パケットあるいは UDP パケットを監視して、ケース 1 または 2 のように状況を判定することにより TCP ベースのワームか、あるいは UDP ベースのワームかを判定し、さらに宛先ポート番号を計測して、その最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する処理をおこなう。ここでは、ケース 1～3 の 3 つの場合について説明したが、さらにさまざまな状況を追加することにより、各パケットの種類に対してワームによる通信か否かを詳細に判定することができる。

#### 【0070】

図 6 は、図 2 に示したワーム判定部 240b がおこなうネットワークセグメント外からのワームスキャンの有無を判定する処理の一例を示す図である。ここでは、SYN ACK パケットに異常が検出された場合を示している。図 6 に示すように、ワーム判定部 240b は、通信ログデータ 230b を参照し、各パケットのパケット数および IP アドレス数が設定データ 230a に記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部 240b は、SYN ACK パケット数の閾値が「10」、送信元 IP アドレス数の閾値が「10」である場合には、計測時間「10:00:35～10:00:36」において SYN ACK パケット数「30」が閾値「10」以上であり、かつ、送信元 IP アドレス数「36」が閾値「10」以上であるので、SYN ACK パケットの異常を検出する。

#### 【0071】

また、ワーム判定部 240b は、通信情報取得部 240a により取得された SYN ACK パケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図 6 の通信ログデータ 230b には、取得された最頻出宛先ポート番号「80」の情報が示されている。最頻出宛先ポート番号の欄に示されている百分率の情報（「90%」および「92%」）は、計測時間内に「SYN ACK パケット数」および「送信元 IP アドレス数」の監視をおこなった全パケットのうち、最頻出宛先ポート番号が「80」番であったパケットの割合を示したものである。

#### 【0072】

その後、ワーム判定部 240b は、上記情報を基にしてワームスキャンの有無を判定し、ワーム判定結果 60 を出力する処理をおこなう。具体的には、ワーム判定部 240b は、SYN パケットを受信した際の応答である SYN ACK パケットがネットワークセグメント A10a 内から閾値より多く送信され、かつ、SYN ACK パケットの送信元 IP アドレス数が閾値より多いため、ネットワークセグメント A を除くネットワーク 12 のコンピュータからネットワークセグメント A10a 内のコンピュータに対してワームによるランダムスキャンがなされていると判定し、そのワーム判定結果 60 を出力する。

#### 【0073】

このワーム判定結果 60 は、スキャン方法、スキャン元 IP アドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン元 IP アドレスは、ランダムスキャンに使用されているパケットを送信しているコンピュータの IP アドレスである。このスキャン元 IP アドレスの情報は、パケットのヘッダより取得することができる。最頻出宛先ポート番号は、通信ログデータ 230b に含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。図 6 の例では、ネットワークセグメント A を除くネットワーク 12 のコンピュータからのランダムスキャンが検出されたので、Web サービスの脆弱性を狙うワームが外部から進入する可能性があることをユーザに通知する。

#### 【0074】



図7は、図2に示したワーム判定部240bがおこなうワーム感染の有無を判定する処理の一例を示す図である。ここでは、SYNパケットに異常が検出された場合を示している。図7に示すように、ワーム判定部240bは、通信ログデータ230bを参照し、各パケットのパケット数およびIPアドレス数が設定データ230aに記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部240bは、SYNパケット数の閾値が「10」、宛先IPアドレス数の閾値が「10」である場合には、計測時間「10:00:37~10:00:38」においてSYNパケット数「22」が閾値「10」以上であり、かつ、宛先IPアドレス数「28」が閾値「10」以上であるので、SYNパケットの異常を検出する。

【0075】

また、ワーム判定部240bは、通信情報取得部240aにより取得されたSYNパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図7の通信ログデータ230bには、取得された最頻出宛先ポート番号「80」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「80」番であったパケットの割合の情報（「94%」および「89%」）とが、SYNパケット数および宛先IPアドレス数のそれぞれの計測項目ごとに示されている。

【0076】

その後、ワーム判定部240bは、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果70を出力する処理をおこなう。具体的には、ワーム判定部240bは、SYNパケットが、ネットワークセグメントA10a内から閾値より多く送信され、かつ、SYNパケットの宛先IPアドレス数が閾値より多いため、ネットワークセグメントA10a内のコンピュータからネットワークセグメントAを除くネットワーク12のコンピュータに対してワームによるランダムスキャンがなされていると判定し、そのワーム判定結果70を出力する。

【0077】

このワーム判定結果70は、スキャン方法、スキャン速度、感染台数、感染コンピュータ名、感染コンピュータIPアドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン速度は、1秒間にスキャンがなされた速度の情報である。感染台数は、ワームに感染した可能性のあるコンピュータの台数であり、感染コンピュータ名は、ワームに感染した可能性のあるコンピュータの名称である。感染コンピュータIPアドレスは、ワームに感染した可能性のあるコンピュータのIPアドレスである。

【0078】

スキャン速度の情報は、単位時間あたりにSYNパケットが送信されたコンピュータ数（宛先IPアドレス数）の情報から算出することができる。また、感染コンピュータIPアドレスは、SYNパケットのヘッダから取得することができる。感染台数の情報は、その感染コンピュータIPアドレスの数から取得することができる。感染コンピュータ名は、IPアドレスとコンピュータ名とを対応付けて記憶したデータベース（図2には、図示していない。）を用意しておくことで取得することができる。最頻出宛先ポート番号は、通信ログデータ230bに含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。

【0079】

図7の例では、ワーム判定部240bは、ネットワークセグメントA10a内からのランダムスキャンが検出され、さらに最頻出宛先ポート番号が「80」番であるので、ネットワークセグメントA10a内のWebサーバが感染した可能性があることをユーザに通知する。また、ワーム判定部240bは、記憶部230のワームデータ230cに記憶されたワームの特徴を参照した結果、類似していると判定されたワームの情報や、ランダムスキャンの対象となったネットワークの情報などをユーザに通知する。

【0080】



図8は、図2に示したワーム判定部240bがおこなうネットワークセグメントA10a外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図である。ここでは、SYN ACKパケットに異常が検出された後、SYNパケットにも異常が検出された場合を示している。図8に示すように、ワーム判定部240bは、通信ログデータ230bを参照し、各パケットのパケット数およびIPアドレス数が設定データ230aに記憶されている閾値以上であるか否かを調べる。

#### 【0081】

たとえば、ワーム判定部240bは、SYN ACKパケット数の閾値が「10」、送信元IPアドレス数の閾値が「10」である場合には、計測時間「10:00:35~10:00:36」においてSYN ACKパケット数「30」が閾値「10」以上であり、かつ、送信元IPアドレス数「36」が閾値「10」以上であるので、SYN ACKパケットの異常を検出する。また、ワーム判定部240bは、SYNパケット数の閾値が「10」、宛先IPアドレス数の閾値が「10」である場合には、計測時間「10:00:37~10:00:38」においてSYNパケット数「22」が閾値「10」以上であり、かつ、宛先IPアドレス数「28」が閾値「10」以上であるので、SYNパケットの異常を検出する。

#### 【0082】

さらに、ワーム判定部240bは、通信情報取得部240aにより取得されたSYN ACKパケットおよびSYNパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図8の通信ログデータ230bには、取得された最頻出宛先ポート番号「80」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「80」番であったパケットの割合の情報（「87%」、「87%」、「89%」および「86%」）とが、SYNパケット数、SYN ACKパケット数、宛先IPアドレス数および送信元IPアドレス数のそれぞれの計測項目ごとに示されている。

#### 【0083】

その後、ワーム判定部240bは、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果80を出力する処理をおこなう。具体的には、ワーム判定部240bは、SYN ACKパケットが、ネットワークセグメントA10a内から閾値より多く送信され、かつ、SYN ACKパケットの送信元IPアドレス数が閾値より多いことから、ネットワークセグメントAを除くネットワーク12のコンピュータからネットワークセグメントA10a内のコンピュータに対してワームによるランダムスキャンがなされていたと判定する。

#### 【0084】

さらに、ワーム判定部240bは、SYNパケットが、ネットワークセグメントA10a内から閾値より多く送信され、かつ、SYNパケットの宛先IPアドレス数が閾値より多いことから、上記ランダムスキャンによりネットワークセグメントA10a内のコンピュータがワームに感染し、そのワームに感染したコンピュータからネットワークセグメントAを除くネットワーク12のコンピュータに対してランダムスキャンがなされていると判定し、そのワーム判定結果80を出力する。

#### 【0085】

このワーム判定結果80は、スキャン方法、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、最頻出宛先ポート番号は、通信ログデータ230bに含まれる最頻出宛先ポート番号である。警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージであり、ネットワークセグメントA10a内のWebサーバが外部からのワーム攻撃により感染した可能性があることをユーザに通知する。

#### 【0086】

図9は、図2に示したワーム判定部がおこなう複数コンピュータのワーム感染の有無を判定する処理の一例を示す図である。ここでは、SYNパケットに異常が検出された後、

再度 S Y N パケットに異常が検出された場合に、再度 S Y N パケットに異常が検出された際の宛先 I P アドレス数が、前回 S Y N パケットに異常が検出された際の宛先 I P アドレス数に比べて増加した状況を示している。

#### 【 0 0 8 7 】

図 9 に示すように、ワーム判定部 2 4 0 b は、通信ログデータ 2 3 0 b を参照し、各パケットのパケット数および I P アドレス数が設定データ 2 3 0 a に記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部 2 4 0 b は、S Y N パケット数の閾値が「1 0」、送信元 I P アドレス数の閾値が「1 0」である場合に、計測時間「1 0：0 0：3 7～1 0：0 0：3 8」において S Y N パケット数「2 2」が閾値「1 0」以上であり、かつ、宛先 I P アドレス数「2 8」が閾値「1 0」以上であるので、S Y N パケットの異常を検出する。また、ワーム判定部 2 4 0 b は、計測時間「1 0：0 0：3 9～1 0：0 0：4 0」において S Y N パケット数「4 9」が閾値「1 0」以上であり、かつ、宛先 I P アドレス数「6 0」が閾値「1 0」以上であるので、S Y N パケットの異常を再度検出する。

#### 【 0 0 8 8 】

さらに、ワーム判定部 2 4 0 b は、通信情報取得部 2 4 0 a により取得された S Y N パケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図 9 の通信ログデータ 2 3 0 b には、取得された最頻出宛先ポート番号「8 0」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「8 0」番であったパケットの割合の情報（「9 2 %」および「9 5 %」）とが、S Y N パケット数および宛先 I P アドレス数のそれぞれの計測項目ごとに示されている。

#### 【 0 0 8 9 】

その後、ワーム判定部 2 4 0 b は、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果 9 0 を出力する処理をおこなう。具体的には、ワーム判定部 2 4 0 b は、S Y N パケットが、ネットワークセグメント A 1 0 a 内から閾値より多く送信され、かつ、S Y N パケットの宛先 I P アドレス数が閾値より多いことから、ネットワークセグメント A 1 0 a 内のコンピュータがワームに感染し、そのワームに感染したコンピュータからネットワークセグメント A を除くネットワーク 1 2 のコンピュータに対してランダムスキャンがなされていると判定する。

#### 【 0 0 9 0 】

また、ワーム判定部 2 4 0 b は、最頻出宛先ポート番号が「8 0」番であり、今回 S Y N パケットに異常が検出された際の宛先 I P アドレス数が、前回 S Y N パケットに異常が検出された際の宛先 I P アドレス数に比べて 2 倍以上増加したので、ネットワークセグメント A 1 0 a 内の複数の W e b サーバがワームに感染したと判定し、そのワーム判定結果 9 0 を出力する。ここでは、宛先 I P アドレス数が 2 倍以上増加した場合に複数の W e b サーバが感染したと判定したが、この倍数は任意に設定できる。

#### 【 0 0 9 1 】

このワーム判定結果 9 0 は、スキャン方法、スキャン速度、感染台数、感染コンピュータ名、感染コンピュータ I P アドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン速度は、1 秒間にスキャンがなされた速度の情報である。感染台数は、ワームに感染したコンピュータの台数であり、感染コンピュータ名は、ワームに感染した可能性のあるコンピュータの名称である。感染コンピュータ I P アドレスは、ワームに感染した可能性のあるコンピュータの I P アドレスである。図 9 の例では、ワームに感染した可能性のある 2 台分の W e b サーバの感染コンピュータ名および感染コンピュータ I P アドレスの情報が示されている。

#### 【 0 0 9 2 】

最頻出宛先ポート番号は、通信ログデータ 2 3 0 b に含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。図 9 の例では、ワーム判定結果 9 0 は、ネットワークセグメント A 1 0 a 内の複数の W e b

サーバがワームに感染した可能性があることを警告メッセージとしてユーザに通知する。

【0093】

図2の説明に戻ると、設定データ変更部240cは、通信情報取得部240a、ワーム判定部240bまたは通信遮断部240dにより参照される設定データ230aに変更がある場合に、ユーザにより入力された新規の設定を受け付け、設定項目の新たな追加や設定項目の更新、あるいはすでに設定されている設定項目の削除などをおこなって設定データ230aを変更する変更部である。また、設定データ変更部240cは、監視していたSYNパケットに異常が検知された場合に、設定データ230aの設定を、初期設定からSYNパケット異常検知後の設定に変更する処理をおこなう。

【0094】

通信遮断部240dは、ワーム判定部240bによりパケット通信がワームによりなされたパケット通信であると判定された場合に、ワームによりなされるパケット通信を遮断する遮断部である。この遮断処理は、図3の設定データ230aにおいて設定項目「遮断」が「ON」である場合におこなわれる。また、この通信遮断部240dは、図3の設定データ230aの設定項目「検知から遮断までの時間」を参照し、そこに設定された時間だけ待機した後、遮断処理を開始する。

【0095】

通信遮断部240dは、具体的には、3通りの方法でワームによるパケット通信を遮断する。図10は、図2に示した通信遮断部240dがおこなうワームによりなされる通信を遮断する遮断処理の例を示す図である。図10に示すように、方法1は、通信遮断部240dが、ワームに感染したと判定されたコンピュータを含んだネットワークセグメントA10a内のすべてのコンピュータからの特定のOutgoing通信（ランダムスキャン）を遮断する方法である。この方法1では、ワームにより送信される通信パケットのプロトコルがTCPベースかUDPベースかの情報や、通信パケットの最頻出宛先ポート番号の情報などを参照してOutgoing通信の遮断をおこなう。その際、通信遮断部240dは、上記情報から特定される通信パケット以外の通信パケットに対しては遮断をおこなわず、通信障害を最小限に抑制する。

【0096】

方法2は、通信遮断部240dが、ネットワークセグメントA10a内のワームに感染したと判定されたコンピュータからの特定のOutgoing通信（ランダムスキャン）を遮断する方法である。この方法2では、ワームにより送信される通信パケットのプロトコルがTCPベースかUDPベースかの情報や、ワームに感染したと判定されたコンピュータを特定する送信元IPアドレス、通信パケットの最頻出宛先ポート番号の情報などを参照してOutgoing通信の遮断をおこなう。その際、通信遮断部240dは、上記情報から特定される通信パケット以外の通信パケットに対しては遮断をおこなわず、通信障害を最小限に抑制する。

【0097】

図11は、ワームによりなされた通信をワーム判定装置20aが遮断する遮断処理を説明する説明図である。図11は、方法1または2によりOutgoing通信の遮断をおこなう場合を示している。図11に示すように、通信遮断部240dは、監視対象としているネットワークセグメントA10aからワームによりなされたOutgoing通信を、ワーム判定装置20aにおいて遮断し、ネットワークセグメントAを除くネットワーク21にワームにより送信された通信パケットが到達するのを防止する。ワームにより送信された通信パケット以外の通信パケットは、通信遮断部240dは、ワーム判定装置20aを通過させ、通信障害を回避する。

【0098】

図10の説明に戻ると、方法3は、方法1または方法2による遮断処理の後、通信遮断部240dが、ワームに感染したと判定されたコンピュータのランダムスキャンを遠隔操作で停止する方法である。具体的には、通信遮断部240dは、ワームに感染したと判定されたコンピュータにアクセスし、ランダムスキャンをおこなっているプロセスを停止さ

せたり、ワームに感染したと判定されたコンピュータのパーソナルファイアウォール等の機能をアクティブに設定し、自装置がおこなっているランダムスキャンを自装置に遮断させる。この方法 3 では、ワームにより送信される通信パケットのプロトコルが T C P ベースか U D P ベースかの情報や、ワームに感染したと判定されたコンピュータを特定する送信元 I P アドレス、通信パケットの最頻出宛先ポート番号の情報などを参照して、遠隔操作によりランダムスキャンの遮断をおこなう。その際、通信遮断部 2 4 0 d は、上記情報から特定される通信パケット以外の通信パケットに対する遮断を、ワームに感染したと判定されたコンピュータがおこなわないように操作し、通信障害を最小限に抑制する。

#### 【 0 0 9 9 】

図 1 2 は、ワームによりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図である。図 1 2 は、方法 3 によりランダムスキャンの遮断をおこなう場合を示している。図 1 2 に示すように、通信遮断部 2 4 0 d は、監視対象としているネットワークセグメント A 1 0 a からのランダムスキャンを、ワームに感染していると判定されたコンピュータ自体に遮断させ、ネットワークセグメント A を除くネットワーク 2 1 にワームにより送信された通信パケットが到達するのを防止する。ワームにより送信された通信パケット以外の通信パケットに対しては、通信遮断部 2 4 0 d は、ワームに感染したと判定されたコンピュータが遮断をおこなわないようにそのコンピュータを操作し、通信障害を回避する。なお、ここでは、方法 1 または 2 による遮断処理の後に方法 3 による遮断処理をおこなうこととしたが、方法 3 による遮断処理を単独でおこなうこととしてもよい。

#### 【 0 1 0 0 】

ここで、特許請求の範囲または後述の付記における「通信情報取得手段」および「通信情報取得手順」・「通信情報取得工程」は、図 2 に示した通信情報取得部 2 4 0 a および通信情報取得部 2 4 0 a がおこなう手順・工程に対応し、「ワーム判定手段」および「ワーム判定手順」・「ワーム判定工程」は、ワーム判定部 2 4 0 b およびワーム判定部 2 4 0 b がおこなう手順・工程に対応し、「設定情報変更手順」は、設定データ変更部 2 4 0 c がおこなう手順に対応し、「通信遮断手段」および「通信遮断手順」・「通信遮断工程」は、通信遮断部 2 4 0 d および通信遮断部 2 4 0 d がおこなう手順・工程に対応する。

#### 【 0 1 0 1 】

また、特許請求の範囲または後述の付記における「情報の取得に係る設定情報」は、図 3 に示した「SYN パケットの計測単位時間」、「SYN ACK パケットの計測単位時間」、「UDP パケットの計測単位時間」、「ICMP ( request ) パケットの計測単位時間」、「ICMP ( reply ) パケットの計測単位時間」、「宛先 IP アドレスの計測単位時間」、「送信元 IP アドレスの計測単位時間」、「宛先ポート番号の参照」、「監視場所」、「監視するネットワークの方向」の各設定項目の情報に対応し、「通信がワームによりなされた通信か否かを規定する判定基準」は、「SYN パケット数の閾値」、「SYN ACK パケット数の閾値」、「UDP パケットの閾値」、「ICMP ( request ) パケットの閾値」、「ICMP ( reply ) パケットの閾値」、「宛先 IP アドレス数の閾値」、「送信元 IP アドレス数の閾値」に対応する。

#### 【 0 1 0 2 】

また、特許請求の範囲または後述の付記における「コンピュータに係る情報」は、図 6、図 7 または図 9 に示したワーム判定結果 6 0、7 0 または 9 0 における「スキャン元 IP アドレス」、「感染台数」、「感染コンピュータ名」および「感染コンピュータ IP アドレス」などに対応し、「通信状況に係る情報」は、図 6 ~ 図 9 に示したワーム判定結果 6 0、7 0、8 0 または 9 0 における「スキャン方法」、「最頻出宛先ポート番号」、警告メッセージ、「スキャン速度」などに対応し、「ログ」は、図 2 に示した通信ログデータ 2 3 0 b に対応する。

#### 【 0 1 0 3 】

つぎに、本実施例に係るワーム判定装置 2 0 a のハードウェア構成について説明する。図 1 3 は、本実施例に係るワーム判定装置 2 0 a のハードウェア構成について説明する。

ロック図である。図13に示すように、このワーム判定装置20aは、キーボード130、ディスプレイ131、CPU132、RAM133、HDD134、ROM136、ネットワークI/F137をバス138で接続した構成となる。

【0104】

ネットワークI/F137は、ネットワークセグメントA10aまたはネットワークセグメントAを除くネットワーク12とワーム判定装置20aとの間での、LAN21またはネットワーク11を介した通信処理をおこなう。

【0105】

また、HDD134が格納および読み出し制御する記憶媒体であるハードディスク(HD)135には、本実施例で示されるワーム判定方法をコンピュータで実行することにより実現するワーム判定プログラム135aが記憶され、実行時にRAM133に読み込まれた後、CPU132によりプログラムが解析され、ワーム判定プロセスの実行がおこなわれる。

【0106】

このワーム判定プロセスが、図2に示した制御部240内の通信情報取得部240a、ワーム判定部240b、設定データ変更部240cおよび通信遮断部240dの各部の機能に対応する。また、設定データ240a、通信ログデータ240bおよびワームデータ240cもHD135に記憶され、RAM133に読み込まれてCPU132により参照される。

【0107】

なお、このワーム判定プログラム135aは、インターネットなどのネットワークを介して配布することができる。また、ワーム判定プログラム135aは、ハードディスク、フレキシブルディスク(FD)、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【0108】

つぎに、本実施例に係るワーム判定処理の処理手順について説明する。図14は、本実施例に係るワーム判定処理の処理手順を示すフローチャートである。図14に示すように、まず、ワーム判定装置20aの設定データ変更部240cは、設定データ230aの変更がある場合に、ユーザにより入力された設定を受け付ける(ステップS1401)。

【0109】

続いて、通信情報取得部240aは、ネットワークセグメントA10a内のコンピュータとネットワークセグメントAを除くネットワーク12内のコンピュータとの間のネットワーク通信を監視し(ステップS1402)、設定データ230aに設定された計測単位時間に基づいてパケットを計測する計測時刻になったか否かを調べる(ステップS1403)。

【0110】

パケットを計測する計測時刻にまだなっていない場合には(ステップS1403, No)、ステップS1402に移行してそれ以降の処理を継続する。パケットを計測する計測時刻になった場合には(ステップS1403, Yes)、通信情報取得部240aは、パケット情報を取得し、取得した情報を通信ログデータ230bに記憶する(ステップS1404)。

【0111】

その後、ワーム判定部240bは、通信情報取得部240aにより取得され、通信ログデータ230bに記憶された情報を基にして、ワームによるパケット通信がなされたか否かの状況を判定する処理をおこなう(ステップS1405)。この状況判定処理については、のちに図15-1および図15-2で詳細に説明する。

【0112】

そして、ワーム判定部240bが、監視対象としているパケット通信がワームによるものではないと判定した場合には(ステップS1406, No)、ステップS1402に移

行してそれ以降の処理を継続する。パケット通信がワームによるものと判定した場合には（ステップ S1406, Yes）、ワーム判定部 240b は、ワームのスキャン方法やスキャン速度、スキャン特徴が類似しているワームの情報などを取得して、出力する処理をおこなう（ステップ S1407）。

【0113】

その後、通信遮断部 240d は、図 10～図 12 で説明したような方法で、ワームによりなされたと判定されるパケット通信を遮断する処理をおこない（ステップ S1408）、このワーム判定処理を終了する。

【0114】

つぎに、図 14 に示した状況判定処理の処理手順について説明する。図 15-1 および図 15-2 は、図 14 に示した状況判定処理の処理手順を示すフローチャート（1）および（2）である。図 15-1 に示すように、まず、ワーム判定部 240b は、通信情報取得部 240a が取得した SYN ACK パケット数が設定データ 230a に設定された SYN ACK パケット数の閾値よりも大きく、かつ、送信元 IP アドレス数が設定データ 230a に設定された送信元 IP アドレス数の閾値よりも大きいかなを調べる（ステップ S1501）。

【0115】

そして、ワーム判定部 240b は、SYN ACK パケット数が SYN ACK パケット数の閾値よりも大きく、かつ、送信元 IP アドレス数が送信元 IP アドレス数の閾値よりも大きい場合には（ステップ S1501, Yes）、ネットワークセグメント A10a 外からのワームスキャンがあると判定し（ステップ S1502）、図 15-2 に示されるように、判定結果を通信ログデータ 230b に記憶して（ステップ S1511）、この状況判定処理を終了する。

【0116】

ステップ S1501 において、SYN ACK パケット数が SYN ACK パケット数の閾値よりも大きいという条件、または、送信元 IP アドレス数が送信元 IP アドレス数の閾値よりも大きいという条件のいずれかが満足されない場合には（ステップ S1501, No）、ワーム判定部 240b は、通信情報取得部 240a が取得した SYN パケット数が設定データ 230a に設定された SYN パケット数の閾値よりも大きく、かつ、宛先 IP アドレス数が設定データ 230a に設定された宛先 IP アドレス数の閾値よりも大きいかなを調べる（ステップ S1503）。

【0117】

そして、SYN パケット数が SYN パケット数の閾値よりも大きいという条件、または、宛先 IP アドレス数が宛先 IP アドレス数の閾値よりも大きいという条件のいずれかが満足されない場合には（ステップ S1503, No）、ネットワークセグメント A10a 外からのワームスキャンはないと判定し（ステップ S1504）、図 15-2 に示されるように、判定結果を通信ログデータ 230b に記憶して（ステップ S1511）、この状況判定処理を終了する。

【0118】

SYN パケット数が SYN パケット数の閾値よりも大きく、かつ、宛先 IP アドレス数が宛先 IP アドレス数の閾値よりも大きい場合には（ステップ S1503, Yes）、ワーム判定部 240b は、ネットワークセグメント A10a 外からのワームスキャンがあると過去の所定の時間内に判定されたかなを調べる（ステップ S1505）。過去の所定の時間内とは、たとえば、5 分前から現時点までの間などである。

【0119】

ネットワークセグメント A10a 外からのワームスキャンがあると過去の所定の時間内に判定された場合には（ステップ S1505, Yes）、ワーム判定部 240b は、図 15-2 に示されるように、ネットワークセグメント A10a 内のコンピュータがネットワークセグメント A10a 外からのパケット通信によりワームに感染したと判定する（ステップ S1506）。

**【0120】**

ネットワークセグメントA10a外からのワームスキャンがあると過去の所定の時間内に判定されなかった場合には（ステップS1505, No）、ワーム判定部240bは、図15-2に示されるように、ネットワークセグメントA10a内のコンピュータがネットワークセグメントA10a外からのパケット通信以外の原因でワームに感染したと判定する（ステップS1507）。ここで、ネットワークセグメントA10a外からのパケット通信以外の原因とは、ネットワークセグメントA10a内のコンピュータが、フレキシブルディスク（FD）やCD-ROMなどの記憶媒体からワームに感染した場合などである。

**【0121】**

ステップS1506またはステップS1507の判定処理ののち、ワーム判定部240bは、今回検出した宛先IPアドレス数が、過去の所定の時間内に検出した宛先IPアドレス数の最大値を2倍した数以上であるか否かを調べる（ステップS1508）。そして、今回検出した宛先IPアドレス数が、過去の所定の時間内に検出した宛先IPアドレス数の最大値を2倍した数以上である場合には（ステップS1508, Yes）、ネットワークセグメントA10a内の複数のコンピュータがワームに感染したと判定し（ステップS1509）、設定データ変更部240cは、通信情報取得部240a、ワーム判定部240bまたは通信遮断部240dにより参照される設定データ230aの設定を、初期設定からSYNパケット異常検知後の設定に変更する処理をおこなう（ステップS1510）。

**【0122】**

ステップS1508において、今回検出した宛先IPアドレス数が、過去の所定の時間内に検出した宛先IPアドレス数の最大値を2倍した数以上でない場合には（ステップS1510）、ステップS1510に移行して、設定データ変更部240cは、設定データ230aの設定を、初期設定からSYNパケット異常検知後の設定に変更する処理をおこなう。その後、ワーム判定部240bは、判定結果を通信ログデータ230bに記憶し、この状況判定処理を終了する。

**【0123】**

上述してきたように、本実施例では、通信情報取得部240aが、設定データ230aに記憶された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、ワーム判定部240bが、通信情報取得部240aにより取得された情報および通信がワームによりなされた通信か否かを規定する、設定データ230aに記憶された判定基準に係る情報に基づいて、通信がワームによりなされた通信か否かを判定することとしたので、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができる。

**【0124】**

また、本実施例では、通信がワームによりなされた通信と判定された場合に、設定データ変更部240cが、設定データ230aに記憶された情報の取得に係る設定情報を変更し、通信情報取得部240aは、変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得することとしたので、通信がワームによりなされた通信と判定された場合に情報の取得に係る設定情報を変更することにより、さらに詳細にワームの挙動を監視することができる。

**【0125】**

また、本実施例では、設定データ変更部240cが、設定データ230aに記憶された情報の取得に係る設定情報に新たに設定する情報の追加、または、すでに情報の取得に係る設定情報に設定されている情報の削除をおこなうこととしたので、情報の取得に係る設定情報を適宜更新することにより、ワームの挙動を適切に監視することができる。

**【0126】**

また、本実施例では、通信がワームによりなされた通信と判定された場合に、設定データ変更部240cが、設定データ230aに記憶された判定基準に係る情報を変更し、通



信情報取得部 240 a により取得された情報および変更された判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、通信がワームによりなされた通信と判定された場合に判定基準に係る情報を変更することにより、さらに厳密に通信がワームによりなされた通信か否かを判定することができる。

【0127】

また、本実施例では、設定データ変更部 240 c が、設定データ 230 a に記憶された判定基準に係る情報に新たに設定する情報の追加、または、すでに判定基準に係る情報に設定されている情報の削除をおこなうこととしたので、判定基準に係る情報を適宜更新することにより、通信がワームによりなされたものか否かを適切に判定できる。

【0128】

また、本実施例では、ワーム判定部 240 b が、通信を監視する監視対象であるネットワークセグメント A10 a からネットワークセグメント A を除くネットワーク 12 に送信される通信パケットのパケット量が増加し、かつ、通信パケットの宛先アドレス数が増加した場合に、ネットワークセグメント A10 a 内のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信がネットワークセグメント A10 a 内のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【0129】

また、本実施例では、ワーム判定部 240 b が、通信を監視する監視対象であるネットワークセグメント A10 a 内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、ネットワークセグメント A10 a からネットワークセグメント A10 a を除くネットワーク 12 に送信される通信パケットの宛先アドレス数が、通信がワームによりなされた通信であると判定する際に、通信情報取得部 240 a により取得されたネットワークセグメント A10 a からネットワークセグメント A10 a を除くネットワーク 12 に送信される通信パケットの宛先アドレス数より増加した場合に、ネットワークセグメント A10 a 内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント A10 a 内の複数のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【0130】

また、本実施例では、ワーム判定部 240 b が、通信を監視する監視対象であるネットワークセグメント A10 a に対してネットワークセグメント A を除くネットワーク 12 から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、通信パケットの送信元アドレス数が増加した場合に、ネットワークセグメント A10 a 外のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント A10 a 外のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【0131】

また、本実施例では、ワーム判定部 240 b が、通信をワームによりなされた通信と判定した場合に、通信をおこなったコンピュータに係る情報をさらに出力することとしたので、出力されたコンピュータに係る情報を基にしてワームに感染している可能性のあるコンピュータを特定することができる。

【0132】

また、本実施例では、ワーム判定部 240 b が、通信をワームによりなされた通信と判定した場合に、通信の通信状況に係る情報をさらに出力することとしたので、出力された通信状況に係る情報を基にしてワームの活動状況を知ることができる。

【0133】

また、本実施例では、ワーム判定部 240 b が、通信がワームによりなされた通信か否かを判定した結果を通信ログデータ 230 b として記憶することとしたので、過去のワームによりなされた通信の状況をいつでも調べることができる。



## 【0134】

また、本実施例では、ワーム判定部240bが、通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るワームデータ230cに記憶された特徴とワームによりなされた通信に係る特徴とを比較することによりワームの種類を推定することとしたので、推定されたワームの種類の情報に基づいてワームの攻撃に適切に対応することができる。

## 【0135】

また、本実施例では、通信遮断部240dが、通信がワームによりなされた通信と判定された場合に、ワームによりなされる通信を遮断することとしたので、ワームの増殖を効果的に抑制することができる。

## 【0136】

また、本実施例では、通信遮断部240dが、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することとしたので、ワームがおこなう処理自体を停止させることにより、ワームの増殖を効果的に抑制することができる。

## 【0137】

また、本実施例では、通信遮断部240dが、ワームによりなされる通信をワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することとしたので、ワームによりなされる通信をワームに感染しているコンピュータに遮断させることにより、ワームの増殖を効果的に抑制することができる。

## 【0138】

さて、これまで本発明の実施の形態について説明したが、本発明は上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施例にて実施されてもよいものである。

## 【0139】

例えば、本実施例では、ここでは、ワーム判定装置20aをネットワークセグメントA10aにLAN21を介して接続することとしたが、本発明はこれに限定されるものではなく、ワーム判定装置20aをネットワークセグメントA10a内のコンピュータに直結することとしてもよい。また、ネットワークセグメントA10aがコンピュータを一台のみ含む場合に、ワーム判定プログラムをそのコンピュータに導入し、そのコンピュータがネットワークセグメントA10aに係る通信を監視してワーム判定処理をおこなうこととしてもよい。

## 【0140】

また、SYNパケットとSYN ACKパケットとを監視する監視する通信パケットの種類として主に取り上げて説明したが、本発明はこれに限定されるものではなく、UDPパケットやICMPパケット、あるいはその他のプロトコルによるパケットにも本発明を同様に適用することができる。

## 【0141】

また、本実施例では、図5～図9に示したような判定方法に基づいて、通信がワームによりなされた通信か否かを判定することとしたが、本発明はこれに限定されるものではなく、通信パケットの通信量および通信パケットの通信アドレスに係る情報を用いた他のさまざまな判定方法を適用することとしてもよい。

## 【0142】

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

## 【0143】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示

のように構成されていることを要しない。すなわち、ワーム判定装置 20 a ~ 20 d の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、ワーム判定装置 20 a ~ 20 d によりおこなわれる各処理機能は、その全部または任意の一部が、CPU および当該 CPU にて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

#### 【0144】

(付記 1) ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させることを特徴とするワーム判定プログラム。

#### 【0145】

(付記 2) 前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記情報の取得に係る設定情報を変更する設定情報変更手順をさらに含み、前記通信情報取得手順は、前記情報取得設定変更手順により変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得することを特徴とする付記 1 に記載のワーム判定プログラム。

#### 【0146】

(付記 3) 前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記判定基準に係る情報を変更する判定基準情報変更手順をさらに含み、前記ワーム判定手順は、前記通信情報取得手順により取得された情報および前記判定基準情報変更手順により変更された判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定することを特徴とする付記 1 または 2 に記載のワーム判定プログラム。

#### 【0147】

(付記 4) 前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする付記 1、2 または 3 に記載のワーム判定プログラム。

#### 【0148】

(付記 5) 前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする付記 4 に記載のワーム判定プログラム。

#### 【0149】

(付記 6) 前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする付記 1 ~ 5 のいずれか 1 つに記載のワーム判定プログラム。

**【 0 1 5 0 】**

(付記 7) 前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、該通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することを特徴とする付記 1 ～ 6 のいずれか 1 つに記載のワーム判定プログラム。

**【 0 1 5 1 】**

(付記 8) 前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされた通信に係る特徴とを比較することにより前記ワームの種類を推定することを特徴とする付記 1 ～ 7 のいずれか 1 つに記載のワーム判定プログラム。

**【 0 1 5 2 】**

(付記 9) 前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする付記 1 ～ 8 のいずれか 1 つに記載のワーム判定プログラム。

**【 0 1 5 3 】**

(付記 1 0) 前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする付記 9 に記載のワーム判定プログラム。

**【 0 1 5 4 】**

(付記 1 1) 前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする付記 9 に記載のワーム判定プログラム。

**【 0 1 5 5 】**

(付記 1 2) ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

**【 0 1 5 6 】**

(付記 1 3) ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、

前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、

を含んだことを特徴とするワーム判定方法。

**【 0 1 5 7 】**

(付記 1 4) ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、

前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、

を備えたことを特徴とするワーム判定装置。

## 【産業上の利用可能性】

【0158】

以上のように、本発明に係るワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置は、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することが必要なワーム判定システムに有用である。

## 【図面の簡単な説明】

【0159】

【図1】本実施例に係るワーム判定システムの概念について説明する概念図である。

【図2】本実施例に係るワーム判定装置の機能的構成について説明する機能ブロック図である。

【図3】図2に示した設定データの一例を示す図である。

【図4】図2に示した通信ログデータの一例を示す図である。

【図5】図2に示したワーム判定部がおこなうパケットの種類ごとのワーム判定処理の例を示す図である。

【図6】図2に示したワーム判定部がおこなうネットワークセグメントA外からのワームスキャンの有無を判定する処理の一例を示す図である。

【図7】図2に示したワーム判定部がおこなうワーム感染の有無を判定する処理の一例を示す図である。

【図8】図2に示したワーム判定部がおこなうネットワークセグメントA外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図である。

【図9】図2に示したワーム判定部がおこなう複数コンピュータのワーム感染の有無を判定する処理の一例を示す図である。

【図10】図2に示した通信遮断部がおこなうワームによりなされる通信を遮断する遮断処理の例を示す図である。

【図11】ワームによりなされた通信をワーム判定装置が遮断する遮断処理を説明する説明図である。

【図12】ワームによりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図である。

【図13】本実施例に係るワーム判定装置のハードウェア構成について説明するブロック図である。

【図14】本実施例に係るワーム判定処理の処理手順を示すフローチャートである。

【図15-1】図14に示した状況判定処理の処理手順を示すフローチャート(1)である。

【図15-2】図14に示した状況判定処理の処理手順を示すフローチャート(2)である。

【図16】ネットワークセグメントの概念を説明する概念図である。

## 【符号の説明】

【0160】

10a~10d、16a~16d      ネットワークセグメント

11      ネットワーク

130      キーボード

131      ディスプレイ

132      CPU

133      RAM

134      HDD

135      HD

135a      ワーム判定プログラム

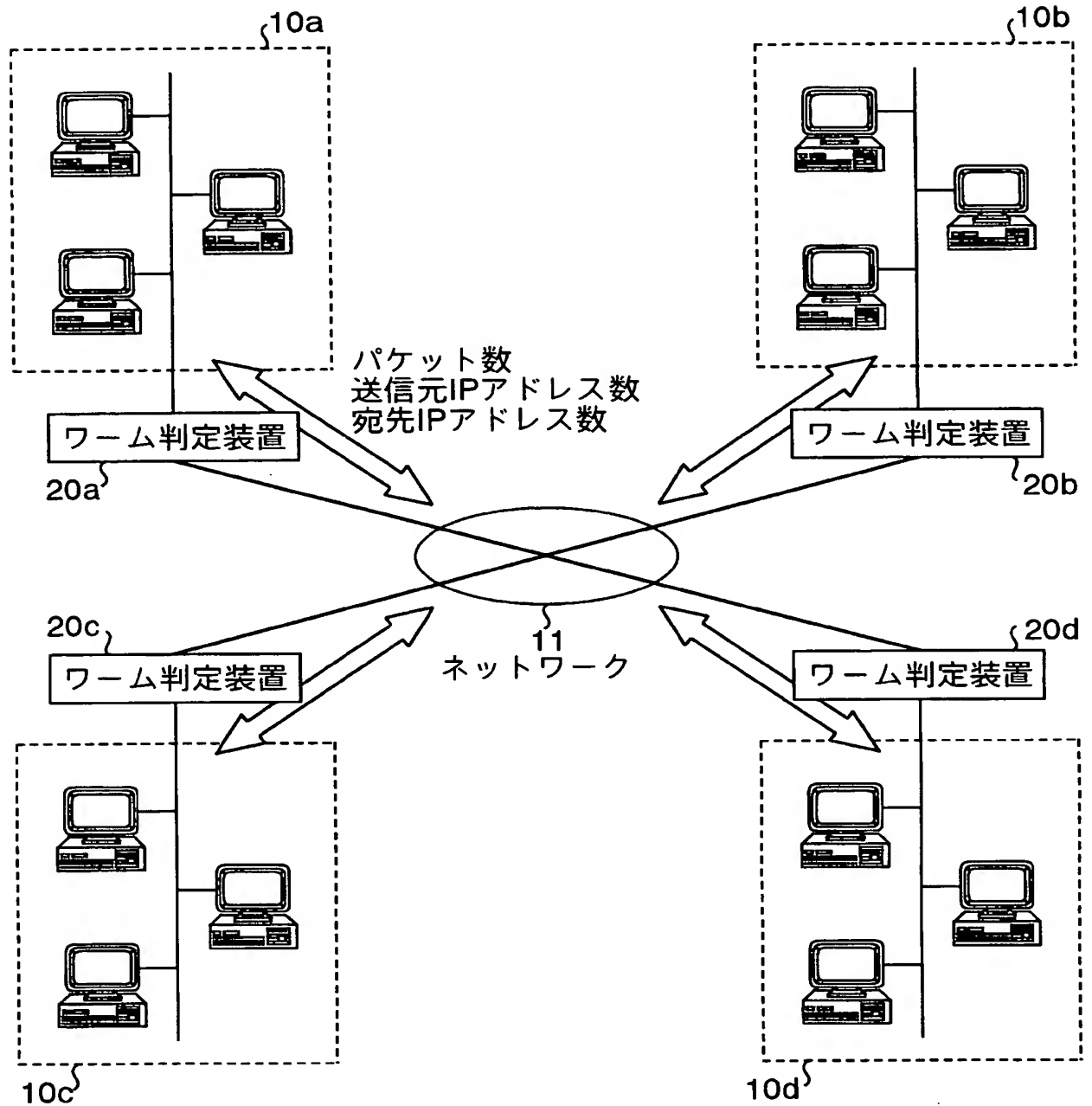
136      ROM

137      ネットワーク I/F

1 3 8      バス  
1 7 a ~ 1 7 c、2 0 a ~ 2 0 d      ワーム判定装置  
2 0 0      インターフェース部  
2 1      L A N  
2 1 0      入力部  
2 2 0      表示部  
2 3 0      記憶部  
2 3 0 a      設定データ  
2 3 0 b      通信ログデータ  
2 3 0 c      ワームデータ  
2 4 0      制御部  
2 4 0 a      通信情報取得部  
2 4 0 b      ワーム判定部  
2 4 0 c      設定データ変更部  
2 4 0 d      通信遮断部  
6 0、7 0、8 0、9 0      ワーム判定結果

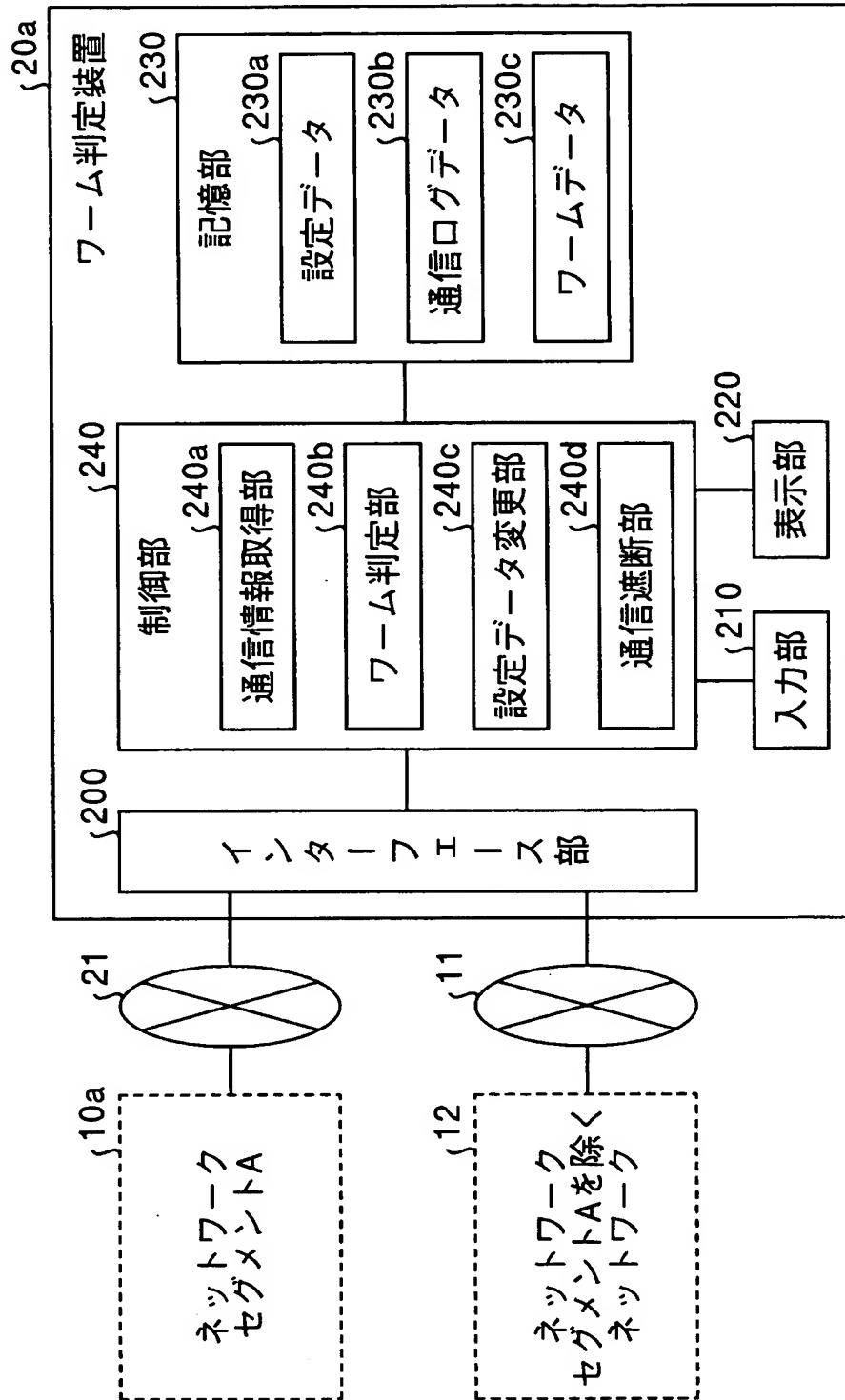
【書類名】 図面  
【図 1】

本実施例に係るワーム判定システムの概念について説明する概念図




本実施例に係るフーム判定装置の機能的構成について説明する機能ブロック図

【図 2】



【図 3】

図2に示した設定データの一例を示す図  


設定項目	初期設置	SYNパケット異常検知後の設定
SYNパケットの計測単位時間	1 sec	0.1 sec
SYN ACKパケットの計測単位時間	1 sec	1 sec
UDPパケットの計測単位時間	1 sec	1 sec
ICMP(request)パケットの計測単位時間	1 sec	1 sec
ICMP(reply)パケットの計測単位時間	1 sec	1 sec
宛先IPアドレスの計測単位時間	1 sec	0.1 sec
送信元IPアドレスの計測単位時間	1 sec	1 sec
宛先ポート番号の参照	OFF	ON
SYNパケット数の閾値	10	2
SYN ACKパケット数の閾値	10	10
UDPパケット数の閾値	10	10
ICMP(request)パケット数の閾値	10	10
ICMP(reply)パケット数の閾値	10	10
宛先IPアドレス数の閾値	10	2
送信元IPアドレス数の閾値	10	10
監視場所	Eth0	Eth0
監視するネットワークの方向	Outgoing	Outgoing
遮断	OFF	ON
検知から遮断までの時間	5 sec	5 sec



図2に示した通信ログデータの一例を示す図

【図4】

230b 通信ログデータ

計測時間	パケット数					IPアドレス数	
	SYN パケット数	SYN ACK パケット数	UDP パケット数	ICMP (request) パケット数	ICMP (replay) パケット数	宛先 IPアドレス数	送信元 IPアドレス数
10:00:34 ~ 10:00:35	4	4	7	0	0	8	9
10:00:35 ~ 10:00:36	5	30	4	1	1	7	36
10:00:36 ~ 10:00:37	5	5	4	2	2	6	8
10:00:37 ~ 10:00:38	22	4	7	0	0	28	8
10:00:38 ~ 10:00:39	4	4	7	0	0	10	9
10:00:39 ~ 10:00:40	49	5	8	0	0	60	10
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 5】


図2に示したワーム判定部がおこなうパケットの種類ごとのワーム判定処理の例を示す図

ケース番号	状況	判定	処理
1	Outgoing通信において SYNパケット数が増加し、 かつ、宛先IPアドレステータス数が増加。	TCPベース のワーム。	最頻出ポート番号からどの サービスを狙ったワームか を検出。80番ポートなら Webサービスである。
2	Outgoing通信において UDPパケット数が増加し、 かつ、宛先IPアドレステータス数が増加。	UDPベース のワーム。	最頻出ポート番号からどの サービスを狙ったワームか を検出。53番ポートなら DNSサービスである。
3	Outgoing通信において ICMP(request)パケット数 が増加し、かつ、宛先IPアド レステータス数が増加。	—	その後のSYNパケットある いはUDPパケットを監視 し、TCPベースのワームか、 あるいはUDPベースのワ ームかを判定し、最頻出ポ ート番号からどのサービ スを狙ったワームかを検出。

【図 6】

図2に示したワーム判定部がおこなうネットワークセグメントA外からのワームスキンの有無を判定する処理の一例を示す図


通信ログデータ  
230b



計測時間	パケット数	IPアドレス数
	SYN ACKパケット数	送信元IPアドレス数
10:00:35 ~ 10:00:36	30	36
最頻出宛先ポート番号	80(90%)	80(92%)



ワーム判定結果  
60



ワーム判定結果

- スキャン方法: SYNパケット
- スキャン元IPアドレス: 192.10.1.14
- 最頻出宛先ポート番号: 80

Webサービスの脆弱性を狙うワームが外部から侵入する可能性があります。

【図7】

図2に示したワーム判定部がおこなう  
ワーム感染の有無を判定する処理の一例を示す図

通信ログデータ  
230b  
↓

計測時間	パケット数	IPアドレス数
	SYNパケット数	宛先IPアドレス数
10:00:37 ~ 10:00:38	22	28
最頻出宛先ポート番号	80(94%)	80(89%)



ワーム判定結果  
70  
↓

ワーム判定結果

- スキャン方法: SYNパケット
- スキャン速度: 10scan/sec
- 感染台数: 1台
- 感染コンピュータ名: lemon
- 感染コンピュータIPアドレス: 192.10.3.5
- 最頻出宛先ポート番号: 80

- ・セグメント内部のWebサーバが感染した可能性があります。
- ・スキャン特徴がBlasterワームに似ています。
- ・ネットワーク192.10.4.0/24にスキャンしました。

図2に示したワーム判定部がおこなうネットワークセグメントA外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図

【図 8】

通信ログデータ  
230b

計測時間	パケット数		IPアドレス数	
	SYNパケット数	SYN ACKパケット数	宛先IPアドレス数	送信元IPアドレス数
10:00:35 ~ 10:00:36	5	30	7	36
10:00:36 ~ 10:00:37	5	5	6	8
10:00:37 ~ 10:00:38	22	4	28	8
最頻出宛先ポート番号	80(87%)	80(87%)	80(89%)	80(86%)

ワーム判定結果  
80

ワーム判定結果  
→ スキャン方法: SYNパケット  
→ 最頻出宛先ポート番号: 80  
セグメント内部のWebサーバが外部から感染した可能性があります。

【図9】

図2に示したワーム判定部がおこなう複数コンピュータの  
ワーム感染の有無を判定する処理の一例を示す図

通信ログデータ  
230b  
↓

計測時間	パケット数	IPアドレス数
	SYNパケット数	宛先IPアドレス数
10:00:37 ~ 10:00:38	22	28
10:00:38 ~ 10:00:39	4	10
10:00:39 ~ 10:00:40	49	60
最頻出宛先ポート番号	80(92%)	80(95%)



ワーム判定結果  
90  
↓

ワーム判定結果

- スキャン方法：SYNパケット
- スキャン速度：10scan/sec
- 感染台数：1台→2台
- 感染コンピュータ名：lemon,apple
- 感染コンピュータIPアドレス：192.10.2.5,192.10.2.11
- 最頻出宛先ポート番号：80

セグメント内部で複数のWebサーバが感染した可能性があります。

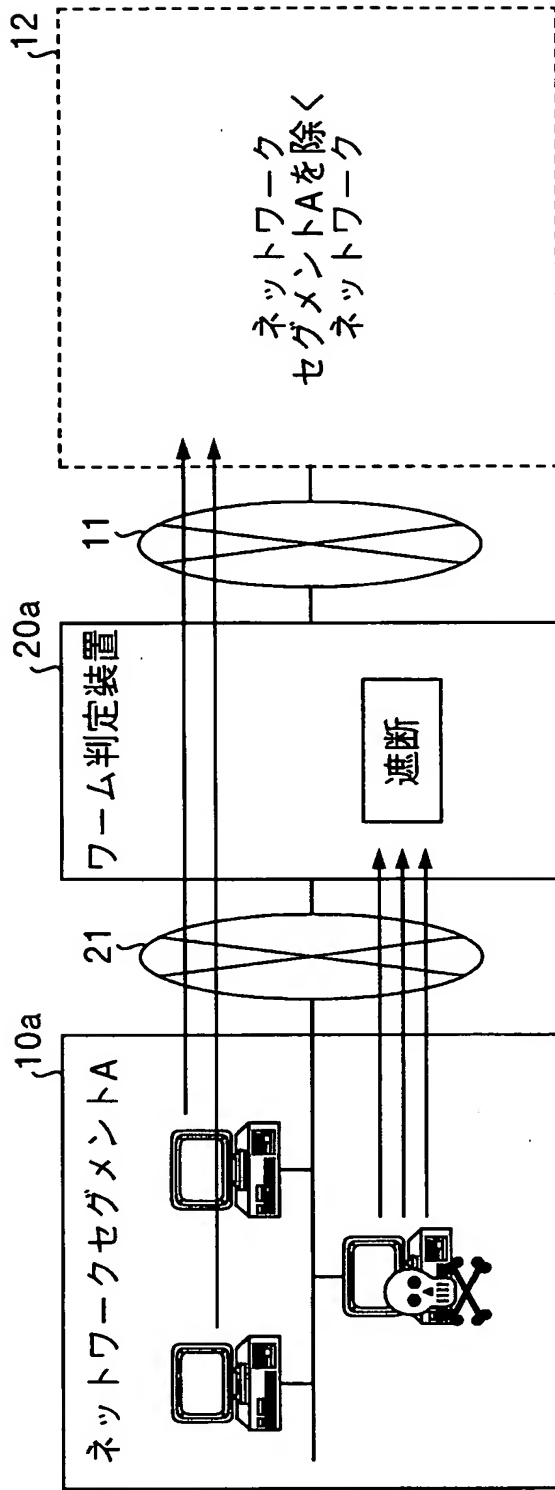
【図 10】

図2に示した通信遮断部がおこなうワームによりなされる通信の遮断処理の例を示す図

方法	処理	参照情報
1	ワームに感染したコンピュータを含んだネットワークセグメントからの特定のOutgoing通信(ランダムスキャン)を遮断。	通信プロトコル(TCP/UDP) 最頻出宛先ポート番号
2	ワームに感染したコンピュータからの特定のOutgoing通信(ランダムスキャン)を遮断。	通信プロトコル(TCP/UDP) 送信元IPアドレス 最頻出宛先ポート番号
3	方法1または2の処理後、ワームに感染したコンピュータのランダムスキャンを遠隔操作で停止(ランダムスキャンをおこなっているプロセスの停止や、パーソナルファイアウォール等による自装置のランダムスキャンの遮断等。)	通信プロトコル(TCP/UDP) 送信元IPアドレス 最頻出宛先ポート番号

【図 11】

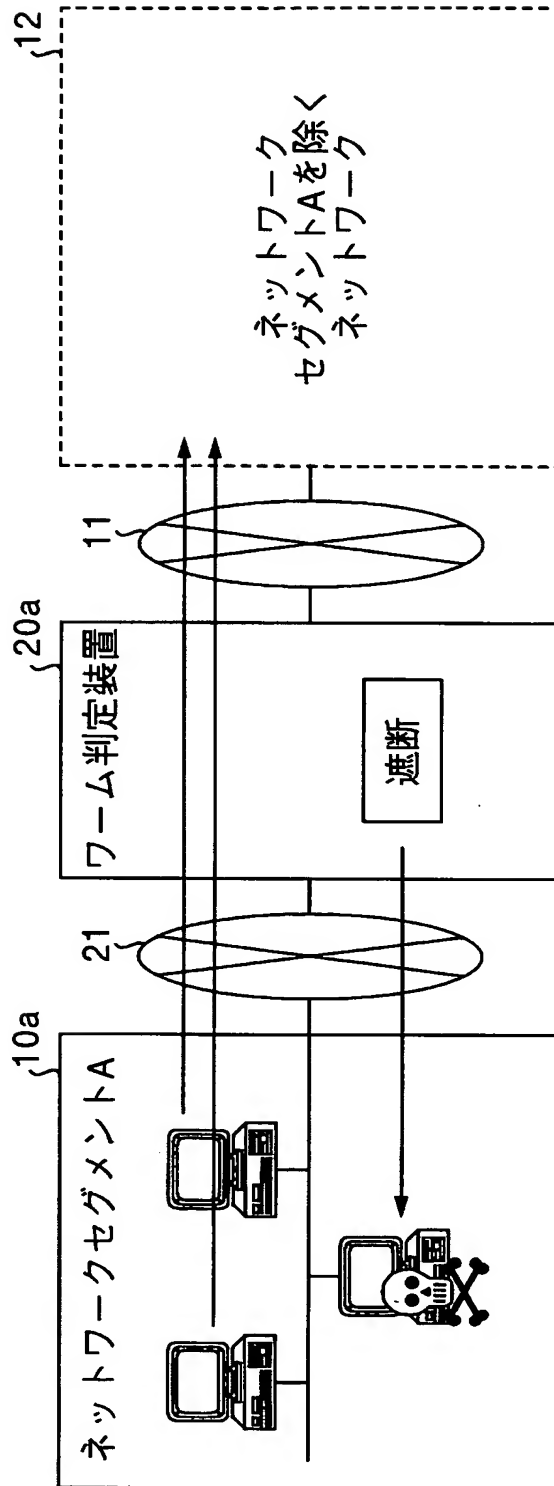
ワームによりなされた通信をワーム判定装置が遮断する遮断処理を説明する説明図





【図 12】

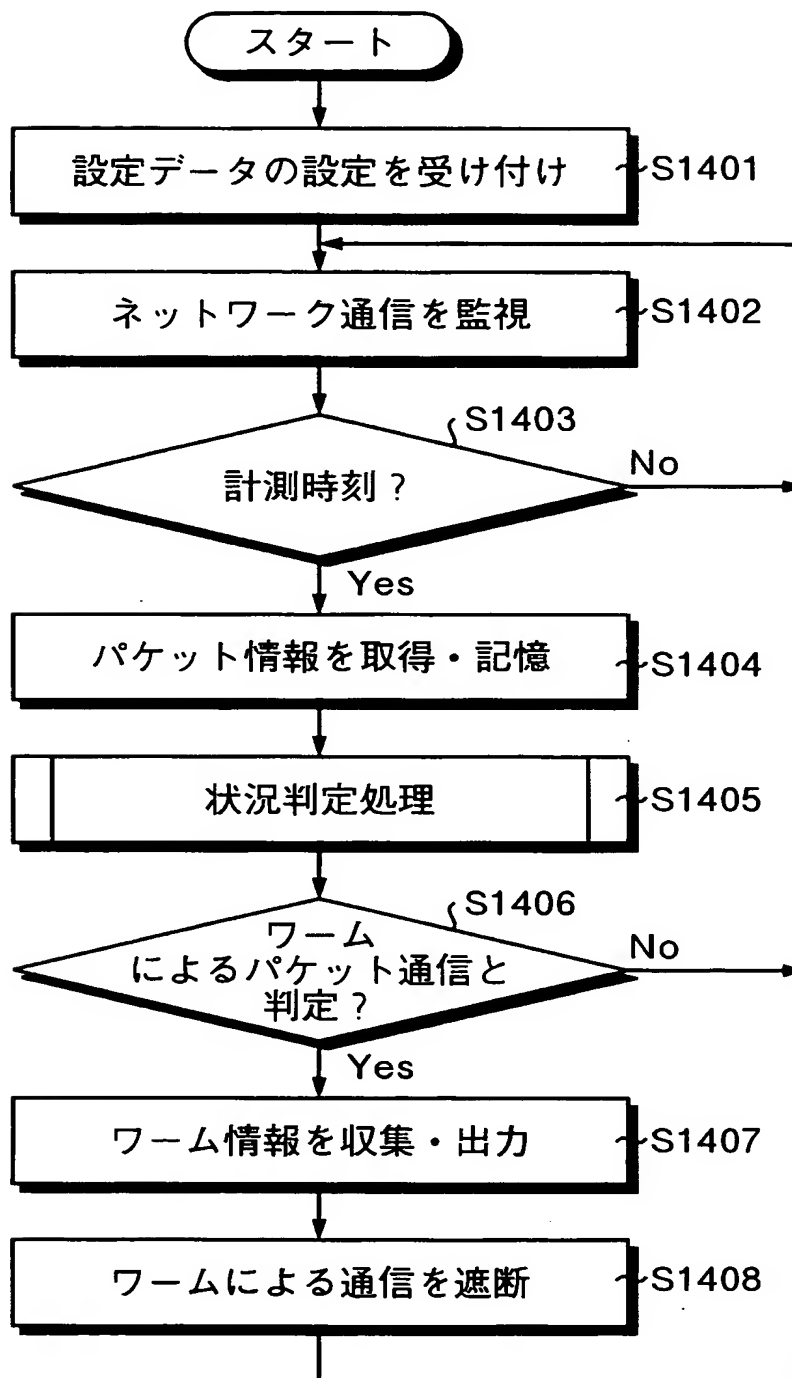
ワームによりなりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図





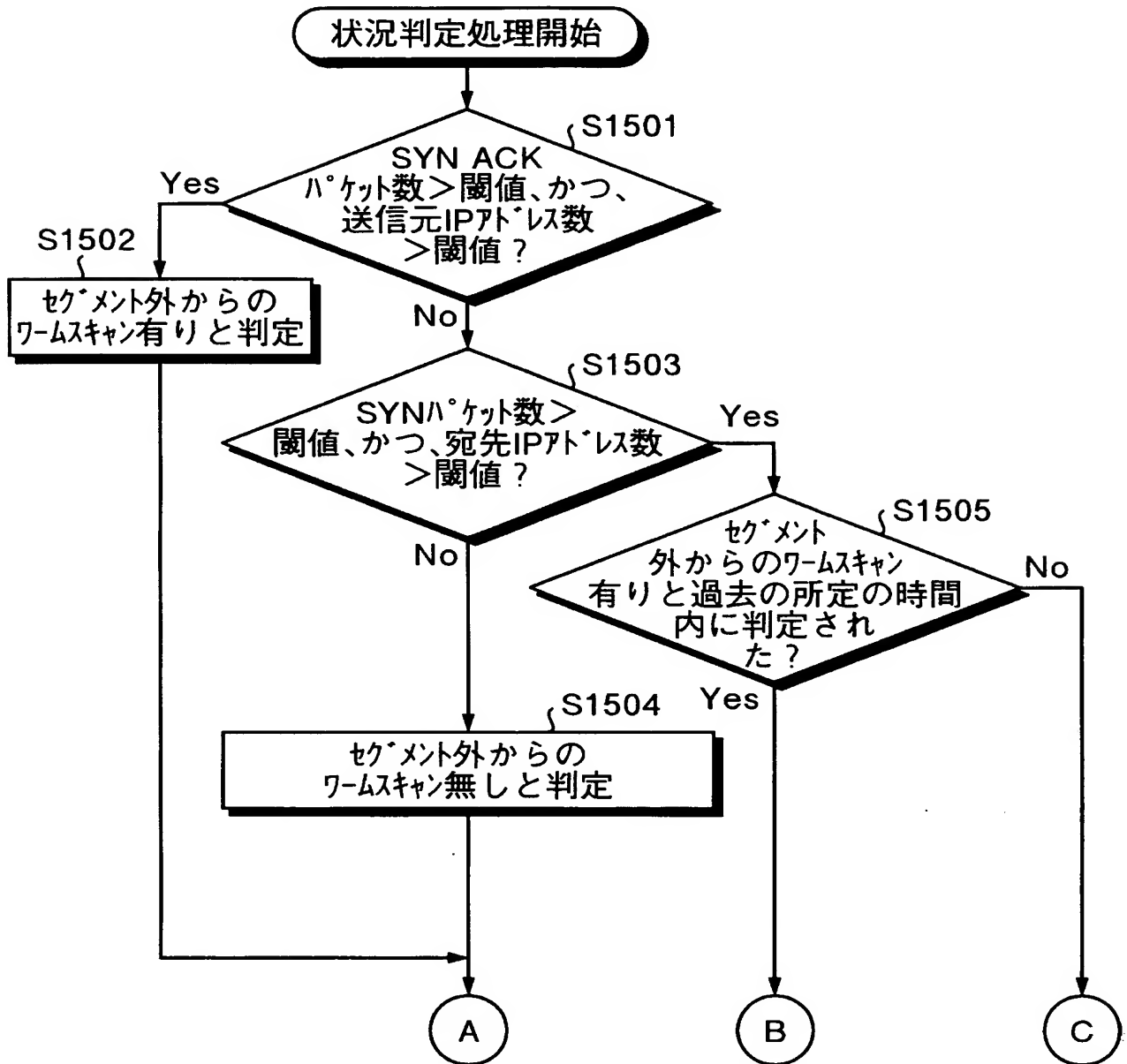
【図 14】

本実施例に係るワーム判定処理の処理手順を示すフローチャート



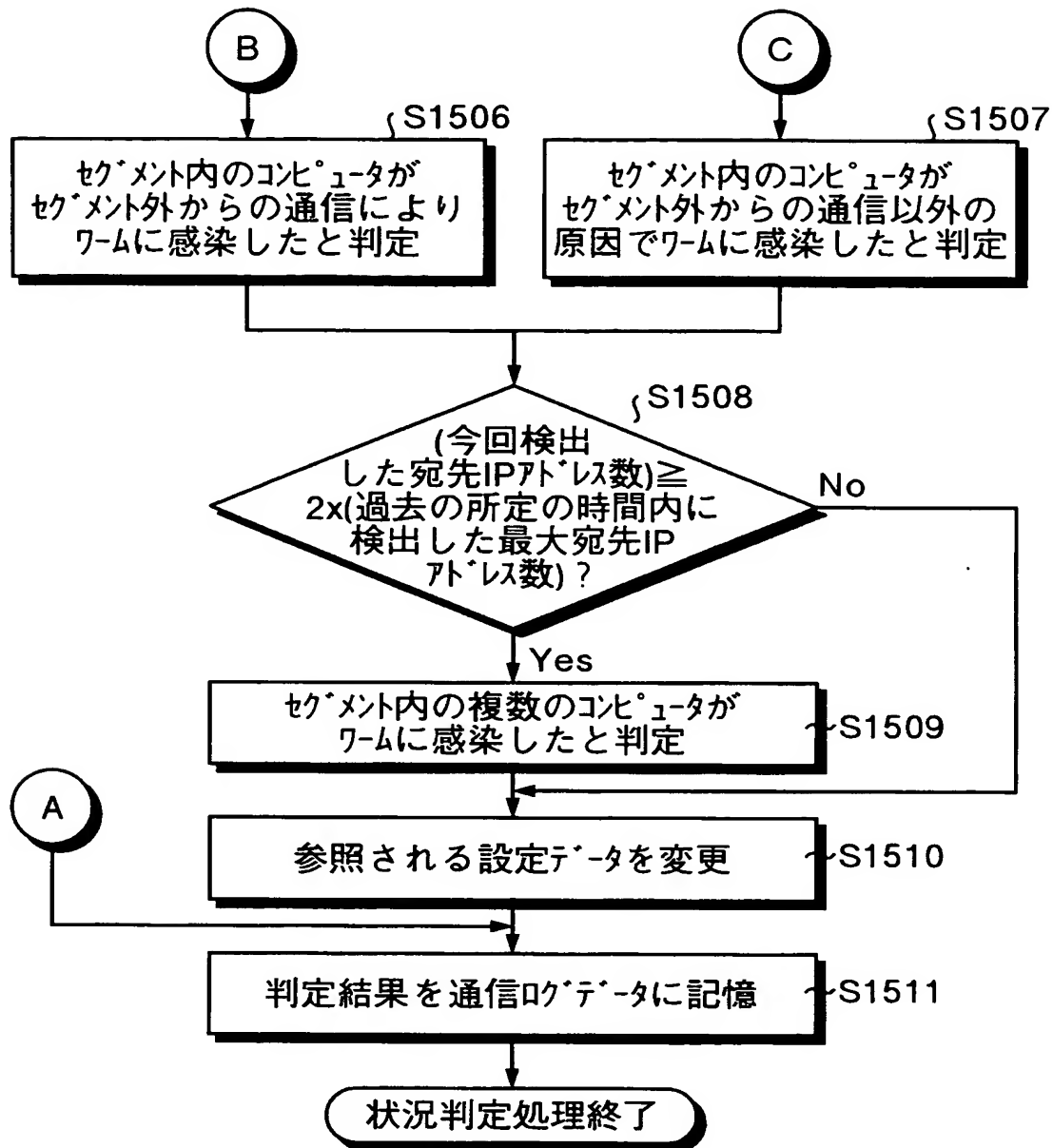
【図15-1】

図14に示した状況判定処理の処理手順を示すフローチャート(1)



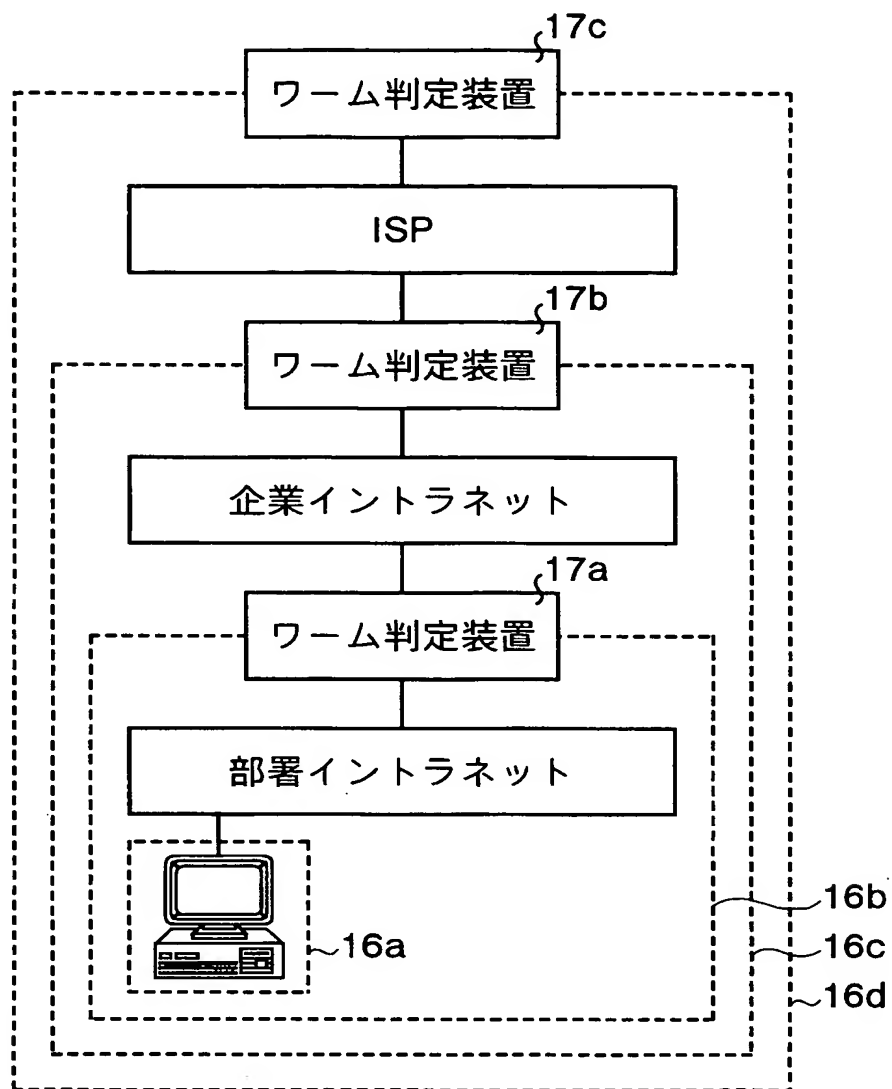
【図15-2】


図14に示した状況判定処理の処理手順を示すフローチャート(2)



【図 16】

ネットワークセグメントの概念を説明する概念図





【書類名】 要約書

【要約】

【課題】 サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定すること。

【解決手段】 通信情報取得部 2 4 0 a が、設定データ 2 3 0 a に記憶された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、ワーム判定部 2 4 0 b が、通信情報取得部 2 4 0 a により取得された情報および通信がワームによりなされた通信か否かを規定する、設定データ 2 3 0 a に記憶された判定基準に係る情報に基づいて、通信がワームによりなされた通信か否かを判定する。

【選択図】

図 2



特願 2 0 0 3 - 3 6 7 2 7 2

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社